Every finite division ring is a field

Chapter 5

Rings are important structures in modern algebra. If a ring R has a multiplicative unit element 1 and every nonzero element has a multiplicative inverse, then R is called a *division ring*. So, all that is missing in R from being a field is the commutativity of multiplication. The best-known example of a non-commutative division ring is the ring of quaternions discovered by Hamilton. But, as the chapter title says, every such division ring must of necessity be infinite. If R is finite, then the axioms force the multiplication to be commutative.

This result which is now a classic has caught the imagination of many mathematicians, because, as Herstein writes: "It is so unexpectedly interrelating two seemingly unrelated things, the number of elements in a certain algebraic system and the multiplication of that system."

Ernst Witt

Theorem. *Every finite division ring R is commutative.*

This beautiful theorem which is usually attributed to MacLagan Wedderburn has been proved by many people using a variety of different ideas. Wedderburn himself gave three proofs in 1905, and another proof was given by Leonard E. Dickson in the same year. More proofs were later given by Emil Artin, Hans Zassenhaus, Nicolas Bourbaki, and many others. One proof stands out for its simplicity and elegance. It was found by Ernst Witt in 1931 and combines two elementary ideas towards a glorious finish.

Proof. Our first ingredient comes from a blend of linear algebra and basic group theory. For an arbitrary element $s \in R$, let C_s be the set $\{x \in R : xs = sx\}$ of elements which commute with s; C_s is called the *centralizer* of s. Clearly, C_s contains 0 and 1 and is a sub-division ring of R. The *center* Z is the set of elements which commute with all elements of R, thus $Z = \bigcap_{s \in R} C_s$. In particular, all elements of Z commute, 0 and 1 are in Z, and so Z is a *finite field*. Let us set $|Z| = q$.

We can regard R and C_s as vector spaces over the field Z and deduce that $|R| = q^n$, where n is the dimension of the vector space R over Z, and similarly $|C_s| = q^{n_s}$ for suitable integers $n_s \geq 1$.

Now let us assume that R is not a field. This means that for *some* $s \in R$ the centralizer C_s is not all of R, or, what is the same, $n_s < n$.

On the set $R^* := R \backslash \{0\}$ we consider the relation

$$r' \sim r \quad :\Longleftrightarrow \quad r' = x^{-1} r x \quad \text{for some } x \in R^*$$

It is easy to check that $\sim$ is an equivalence relation. Let

$$A_s := \{x^{-1}sx : x \in R^*\}$$

be the equivalence class containing s. We note that $|A_s| = 1$ precisely when s is in the center Z. So by our assumption, there are classes A_s with $|A_s| \geq 2$. Consider now for $s \in R^*$ the map $f_s : x \longmapsto x^{-1}sx$ from R^* onto A_s. For $x, y \in R^*$ we find

$$\begin{aligned} x^{-1}sx = y^{-1}sy &\iff (yx^{-1})s = s(yx^{-1}) \\ &\iff yx^{-1} \in C_s^* \iff y \in C_s^* x, \end{aligned}$$

for $C_s^* := C_s \backslash \{0\}$, where $C_s^* x = \{zx : z \in C_s^*\}$ has size $|C_s^*|$. Hence any element $x^{-1}sx$ is the image of precisely $|C_s^*| = q^{n_s} - 1$ elements in R^* under the map f_s, and we deduce $|R^*| = |A_s|\,|C_s^*|$. In particular, we note that

$$\frac{|R^*|}{|C_s^*|} = \frac{q^n - 1}{q^{n_s} - 1} = |A_s| \quad \text{is an } \textit{integer} \text{ for all } s.$$

We know that the equivalence classes partition R^*. We now group the central elements Z^* together and denote by $A_1, \ldots, A_t$ the equivalence classes containing more than one element. By our assumption we know $t \geq 1$. Since $|R^*| = |Z^*| + \sum_{k=1}^{t} |A_k|$, we have proved the so-called *class formula*

$$q^n - 1 = q - 1 + \sum_{k=1}^{t} \frac{q^n - 1}{q^{n_k} - 1}, \tag{1}$$

where we have $1 < \frac{q^n-1}{q^{n_k}-1} \in \mathbb{N}$ for all k.

With (1) we have left abstract algebra and are back to the natural numbers. Next we claim that $q^{n_k} - 1 \mid q^n - 1$ implies $n_k \mid n$. Indeed, write $n = an_k + r$ with $0 \leq r < n_k$, then $q^{n_k} - 1 \mid q^{an_k + r} - 1$ implies

$$q^{n_k} - 1 \mid (q^{an_k+r} - 1) - (q^{n_k} - 1) = q^{n_k}(q^{(a-1)n_k+r} - 1),$$

and thus $q^{n_k} - 1 \mid q^{(a-1)n_k+r} - 1$, since q^{n_k} and $q^{n_k} - 1$ are relatively prime. Continuing in this way we find $q^{n_k} - 1 \mid q^r - 1$ with $0 \leq r < n_k$, which is only possible for $r = 0$, that is, $n_k \mid n$. In summary, we note

$$n_k \mid n \quad \text{for all } k. \tag{2}$$

Now comes the second ingredient: the complex numbers $\mathbb{C}$. Consider the polynomial $x^n - 1$. Its roots in $\mathbb{C}$ are called the *n-th roots of unity*. Since $\lambda^n = 1$, all these roots λ have $|\lambda| = 1$ and lie therefore on the unit circle of the complex plane. In fact, they are precisely the numbers $\lambda_k = e^{\frac{2k\pi i}{n}} = \cos(2k\pi/n) + i\sin(2k\pi/n)$, $0 \leq k \leq n - 1$ (see the box on the next page). Some of the roots λ satisfy $\lambda^d = 1$ for $d < n$; for example, the root $\lambda = -1$ satisfies $\lambda^2 = 1$. For a root λ, let d be the smallest positive exponent with $\lambda^d = 1$, that is, d is the order of λ in the group of the roots of unity. Then $d \mid n$, by Lagrange's theorem ("the order of every element of

a group divides the order of the group" — see the box in Chapter 1). Note that there are roots of order n, such as $\lambda_1 = e^{\frac{2\pi i}{n}}$.

Roots of unity

Any complex number $z = x + iy$ may be written in the "polar" form

$$z = re^{i\varphi} = r(\cos\varphi + i\sin\varphi),$$

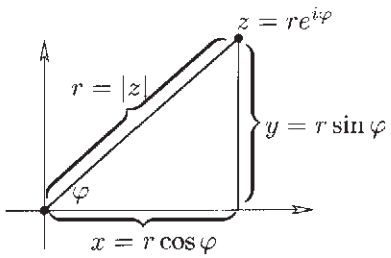
where $r = |z| = \sqrt{x^2 + y^2}$ is the distance of z to the origin, and φ is the angle measured from the positive x-axis. The n-th roots of unity are therefore of the form

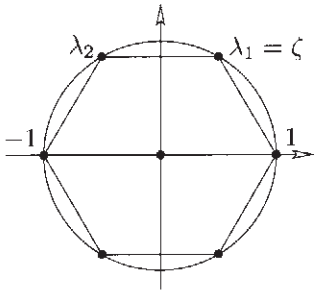
$$\lambda_k = e^{\frac{2k\pi i}{n}} = \cos(2k\pi/n) + i\sin(2k\pi/n), \qquad 0 \le k \le n-1,$$

since for all k

$$\lambda_k^n = e^{2k\pi i} = \cos(2k\pi) + i\sin(2k\pi) = 1.$$

We obtain these roots geometrically by inscribing a regular n-gon into the unit circle. Note that $\lambda_k = \zeta^k$ for all k, where $\zeta = e^{\frac{2\pi i}{n}}$. Thus the n-th roots of unity form a cyclic group $\{\zeta, \zeta^2, \ldots, \zeta^{n-1}, \zeta^n = 1\}$ of order n.





The roots of unity for $n = 6$

Now we group all roots of order d together and set

$$\phi_d(x) := \prod_{\lambda \text{ of order } d} (x - \lambda).$$

Note that the definition of $\phi_d(x)$ is independent of n. Since every root has some order d, we conclude that

$$x^n - 1 = \prod_{d \mid n} \phi_d(x). \tag{3}$$

Here is the crucial observation: The *coefficients* of the polynomials $\phi_n(x)$ are *integers* (that is, $\phi_n(x) \in \mathbb{Z}[x]$ for all n), where in addition the constant coefficient is either 1 or -1.

Let us carefully verify this claim. For $n = 1$ we have 1 as the only root, and so $\phi_1(x) = x - 1$. Now we proceed by induction, where we assume $\phi_d(x) \in \mathbb{Z}[x]$ for all $d < n$, and that the constant coefficient of $\phi_d(x)$ is 1 or -1. By (3),

$$x^n - 1 = p(x)\,\phi_n(x) \tag{4}$$

where $p(x) = \sum_{j=0}^{\ell} p_j x^j$, $\phi_n(x) = \sum_{k=0}^{n-\ell} a_k x^k$, with $p_0 = 1$ or $p_0 = -1$.

Since $-1 = p_0 a_0$, we see $a_0 \in \{1, -1\}$. Suppose we already know that $a_0, a_1, \ldots, a_{k-1} \in \mathbb{Z}$. Computing the coefficient of x^k on both sides of (4)

we find

$$\sum_{j=0}^{k} p_j a_{k-j} \;=\; \sum_{j=1}^{k} p_j a_{k-j} + p_0 a_k \;\in\; \mathbb{Z}.$$

By assumption, all $a_0, \ldots, a_{k-1}$ (and all p_j) are in $\mathbb{Z}$. Thus $p_0 a_k$ and hence a_k must also be integers, since p_0 is 1 or -1.

We are ready for the *coup de grâce*. Let $n_k \mid n$ be one of the numbers appearing in (1). Then

$$x^n - 1 \;=\; \prod_{d \mid n} \phi_d(x) \;=\; (x^{n_k} - 1)\phi_n(x) \prod_{d \mid n,\, d \nmid n_k,\, d \neq n} \phi_d(x).$$

We conclude that in $\mathbb{Z}$ we have the divisibility relations

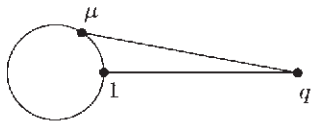
$$\phi_n(q) \mid q^n - 1 \qquad \text{and} \qquad \phi_n(q) \,\Big|\, \frac{q^n - 1}{q^{n_k} - 1}. \tag{5}$$

Since (5) holds for all k, we deduce from the class formula (1)

$$\phi_n(q) \mid q - 1,$$

but this cannot be. Why? We know $\phi_n(x) = \prod(x - \lambda)$ where λ runs through all roots of $x^n - 1$ of order n. Let $\widetilde{\lambda} = a + ib$ be one of those roots. By $n > 1$ (because of $R \neq Z$) we have $\widetilde{\lambda} \neq 1$, which implies that the real part a is smaller than 1. Now $|\widetilde{\lambda}|^2 = a^2 + b^2 = 1$, and hence

$$\begin{aligned} |q - \widetilde{\lambda}|^2 \;&=\; |q - a - ib|^2 \;=\; (q-a)^2 + b^2 \\ &=\; q^2 - 2aq + a^2 + b^2 \;=\; q^2 - 2aq + 1 \\ &>\; q^2 - 2q + 1 \qquad \text{(because of } a < 1\text{)} \\ &=\; (q-1)^2, \end{aligned}$$



$|q - \mu| > |q - 1|$

and so $|q - \widetilde{\lambda}| > q - 1$ holds for *all* roots of order n. This implies

$$|\phi_n(q)| \;=\; \prod_{\lambda} |q - \lambda| > q - 1,$$

which means that $\phi_n(q)$ cannot be a divisor of $q - 1$, contradiction and end of proof. □

References

[1] L. E. DICKSON: *On finite algebras,* Nachrichten der Akad. Wissenschaften Göttingen Math.-Phys. Klasse (1905), 1-36; Collected Mathematical Papers Vol. III, Chelsea Publ. Comp, The Bronx, NY 1975, 539-574.

[2] J. H. M. WEDDERBURN: *A theorem on finite algebras,* Trans. Amer. Math. Soc. **6** (1905), 349-352.

[3] E. WITT: *Über die Kommutativität endlicher Schiefkörper,* Abh. Math. Sem. Univ. Hamburg **8** (1931), 413.